

# Notice of Allowability

Application No.

10/067,950

Examiner

Andrew L. Nalven

Applicant(s)

KAMBAYASHI, TORU

Art Unit

2134

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment submitted 11/14/2006.
2. ☒ The allowed claim(s) is/are 18-25.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All b) ☐ Some\* c) ☐ None of the:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).


\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date 5/26/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
KAMBIZ ZAND  
PRIMARY EXAMINER

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Surinder Sachar (Registration No. 34,423) on 26 January 2007.

The application has been amended as follows:

Claims 5-8 and 11-17 are canceled.

Claim 18. A revoke control method for revoking at least one of a plurality of content utilizing devices, each of the content utilizing devices being assigned a device ID and assigned a set of device keys according to the device ID, the device ID being formed of numerals each indicating a position of each of the device keys of the set in each one dimensional array of a device key matrix in which device keys are arranged in a two dimensional manner, and the device ID indicating a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix, the method comprising:

preparing the device key matrix;

Art Unit: 2134

inputting a revoke target path, which is a path to be revoked in the trees and formed of numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

calculating a boundary set of paths except for the revoke target path in the trees, each of the paths of the boundary set being formed of one or more numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

calculating a path function value corresponding to each of the paths of the boundary set based on each device key indicated by each numeral of the each of the paths of the boundary set, to obtain a plurality of path function values corresponding to the paths of the boundary set;

encrypting a master key by using each of the path function values, to obtain a plurality of encrypted data items corresponding to the paths of the boundary set;

generating revoke control data including the encrypted data items; and

outputting the revoke control data to each of the content utilizing devices; and

decrypting, by each content utilizing device whose device ID indicates one of the boundary set of paths, ~~configured to decrypt~~ one of the encrypted data items by using a path function value calculated based on one or more device keys of the set assigned to the each content utilizing device.

1. Claims 18-25 are allowed.

Art Unit: 2134

2. The following is an examiner's statement of reasons for allowance: The cited prior art, Shimbo et al US Patent No. 6,185,680 and "Matrix Digital Signature for Use with the data encryption algorithm" fails to teach or suggest decrypting, by each content utilizing device whose device ID indicates one of the boundary set of paths, one of the encrypted data items by using a path function value calculated based on one or more device keys of the set assigned to the each content utilizing device. As a result, the cited prior art fails to anticipate or render obvious the above cited claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven



KAMBIZ ZAND  
PRIMARY EXAMINER